ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.7, July 2010, pp.1758−1767
doi: 10.3724/SP.J.1001.2010.03731

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一类代数免疫度达到最优的布尔函数的构造*

孟 强[1+], 陈鲁生[1], 符方伟[2]

[1](南开大学 数学科学学院,天津 300071)

[2](南开大学 陈省身数学研究所,天津 300071)

Construction of Boolean Functions with Maximum Algebraic Immunity

MENG Qiang[1+], CHEN Lu-Sheng[1], FU Fang-Wei[2]

[1](School of Mathematical Science, Nankai University, Tianjin 300071, China)

[2](Chern Institute of Mathematics, Nankai University, Tianjin 300071, China)

+ Corresponding author: E-mail: nkmengq@gmail.com

Meng Q, Chen LS, Fu FW. Construction of Boolean functions with maximum algebraic immunity. *Journal of Software*, 2010,21(7):1758−1767. http://www.jos.org.cn/1000-9825/3731.htm

Abstract: This paper presents a construction of Boolean functions with the maximum algebraic immunity on even number of variables. It also gives a construction of balanced rotation symmetric Boolean functions with the maximum algebraic immunity on even number of variables. This paper uses some results of linear algebra and enumerative combinatorics in the constructions. These functions have strong resistance against algebraic attacks. The balanced rotation symmetric Boolean functions constructed can also be used in the construction of safer hashing functions.

Key words: algebraic attack; algebraic immunity; nonlinearity; rotation symmetric; Boolean function

摘 要: 给出了一种具有最优代数免疫度的偶数元布尔函数的构造,同时还给出了一种具有最优代数免疫度的平衡旋转对称偶数元布尔函数的构造.在构造过程中用到了线性代数和组合计数中的有关结论,这些函数对代数攻击均有很强的抵抗能力.构造的平衡旋转对称布尔函数还可用在 Hash 算法的轮函数中,增加了算法的安全性.

关键词: 代数攻击;代数免疫度;非线性度;旋转对称;布尔函数

中图法分类号: TP309 **文献标识码**: A

在 1998 年的欧密会上,首次出现了旋转对称布尔函数(简称 RotS(rotation symmetric)函数)的概念,这类函数在密码学中有着广泛的应用.RotS 函数提供更有效率的计算,因此它们被用在诸如 MD4,MD5 以及 HAVAL 这些 Hash 算法的轮函数中.通过实验验证人们发现,RotS 函数还具有很好的密码学性质[1,2].同时,RotS 函数($\approx 2^{\frac{2^n}{n}}$ 个)相比相同变量的全体布尔函数(共 2^{2^n} 个)所含有的函数数目较少,更有利于我们通过计算机高效率地发现新的具有更佳密码学性质的 RotS 函数.

最近,代数攻击方法的出现使得代数免疫度成为衡量布尔函数抵抗代数攻击的一个重要指标.布尔函数的

* Supported by the National Natural Science Foundation of China under Grant No.60872025 (国家自然科学基金)
Received 2009-04-14; Revised 2009-07-06; Accepted 2009-08-26

代数免疫度是为了描述基于线性反馈移位寄存器的流密码体制抵抗代数攻击的性质而提出的.低代数免疫度的布尔函数可以使攻击者用较少的计算代价来获得系统的初始密钥,具有高代数免疫度的布尔函数能够更好地抵抗代数攻击.文献[3]告诉我们,任意一个 n 元布尔函数的代数免疫度 $\leqslant \left\lceil \frac{n}{2} \right\rceil$.这里,$\lceil x \rceil$表示不小于 x 的最小整数.因此,具有最优代数免疫度 $\left\lceil \frac{n}{2} \right\rceil$ 的布尔函数是密码学中的一类重要的函数.

到目前为止,已有一些关于具有最优代数免疫度的布尔函数的构造.由于奇数个变量具有最优代数免疫度的布尔函数同时也满足平衡性[3],而偶数个变量的函数却没有相应的性质.因此,大多数文献仅给出奇数元具有最优代数免疫度的布尔函数的构造,对于偶数元具有最优代数免疫度的布尔函数的构造却很少出现.例如,文献[4–6]给出了一些关于奇数个变量的具有最优代数免疫度的布尔函数的构造,这些函数满足平衡性.文献[3]给出了一种偶数元具有最优代数免疫度的布尔函数的构造,该函数具有较大的非线性度.但是,这种函数不满足平衡性.这里我们给出了一种具有最优代数免疫度的偶数元布尔函数的构造,同时,还给出了具有最优代数免疫度的平衡偶数元 RotS 函数的构造,而且我们构造的函数还具有较大的非线性度.

本文第 1 节介绍相关概念.第 2 节给出具有最优代数免疫度的偶数元布尔函数的构造.第 3 节讨论推论 1 中给出的函数的非线性度.第 4 节利用第 2 节中的结果给出具有最优代数免疫度的平衡偶数元 RotS 函数的构造.

1 概 念

令 F_2^n 是二元域 F_2 上的 n 维向量空间,B_n 为所有 n 元布尔函数组成的集合.对于任意一个集合 A,用符号 $\#A$ 表示集合 A 内元素的个数.设 $(a_1,...,a_n) \in F_2^n$,我们定义变换 $\rho_n^k (1 \leqslant k \leqslant n)$ 为

$$\rho_n^k (a_1,...,a_n) = (\rho_n^k (a_1),...,\rho_n^k (a_n)),$$

其中,

$$\rho_n^k (a_i) = \begin{cases} a_{i+k}, & i+k \leqslant n \\ a_{i+k-n}, & i+k > n \end{cases}.$$

对于 $a = (a_1,...,a_n) \in F_2^n$,如果 $i>n$,我们约定 $a_i = a_{i_0}$,其中,i_0 满足 $i \equiv i_0 (\mathrm{mod}\ n)$ 与 $1 \leqslant i_0 \leqslant n$.这给我们接下来的讨论带来了方便.例如,在这种约定下,$\rho_n^k (a_i) = a_{i+k}$.我们定义向量的加法:

$$a \oplus b = (a_1 \oplus b_1,\ldots,a_n \oplus b_n),$$

其中,

$$a = (a_1,\ldots,a_n), b = (b_1,...,b_n) \in F_2^n.$$

定义 1. 布尔函数 f 是旋转对称函数当且仅当对任意的输入 $(a_1,...,a_n) \in F_2^n$,$f(\rho_n^k (a_1,...,a_n)) = f(a_1,...,a_n)$ 对 $1 \leqslant k \leqslant n$ 成立.

设 $a = (a_1,...,a_n) \in F_2^n$,我们称集合 $G_n(a) = \{\rho_n^k (a) \mid 1 \leqslant k \leqslant n\}$ 为向量 a 在变换 $\rho_n^k (1 \leqslant k \leqslant n)$ 下生成的轨道.显然,$G_n(a) = G_n(\rho_n^k (a))(1 \leqslant k \leqslant n)$,从而有两个轨道要么相等,要么不相交.我们定义 $T_n(a)$ 为满足 $(a_1,a_2,\ldots,a_n) = (a_{1+t},a_{2+t},\ldots,a_{n+t})$ 的所有正整数 t 中最小的正整数,$T_n(a)$ 称为向量 a 的周期.易见 $T_n(a) = \#G_n(a)$,且对任何满足等式 $(a_1,a_2,\ldots,a_n) = (a_{1+t},a_{2+t},\ldots,a_{n+t})$ 的正整数 t 均有 $T_n(a) \mid t$.特别地,$T_n(a) \mid n$.

从上面的定义中可以看出,f 是 RotS 函数当且仅当其在每个轨道上有相同的函数取值.

设 E 是 F_2^n 的任意一个子集合,记 $\overline{E} = \{\overline{x} \mid x \in E\}$.其中,$x=(x_1,\ldots,x_n)$,$\overline{x} = (x_1 \oplus 1,...,x_n \oplus 1)$.

易见,如果 $G_n(a)$ 是一个轨道,那么 $\overline{G_n(a)}$ 仍是一个轨道,并且 $\#\overline{G_n(a)} = \#G_n(a), \overline{G_n(a)} = G_n(\overline{a})$.$\overline{G_n(a)}$ 称为轨道 $G_n(a)$ 的共轭轨道.如果 $G_n(a) = \overline{G_n(a)}$ 成立,则 $G_n(a)$ 称为自共轭轨道.

任何 n 元布尔函数 $f(x_1,\ldots,x_n)$ 可以表示为

$$f(x_1,...,x_n)=a_0\bigoplus_{1\leqslant i\leqslant n}a_ix_i\bigoplus_{1\leqslant i<j\leqslant n}a_{ij}x_ix_j\oplus...\oplus a_{12...n}x_1x_2...x_n,$$

其中,系数 $a_0,a_i,a_{ij},\ldots,a_{12\ldots n}\in F_2$.这种表示称为 f 的代数正规型(简称 ANF(algebraic norm form)).布尔函数 f 的次数定义为 f 的 ANF 中具有非零系数的乘积项中的最大次数,记为 deg(f).

函数 f 的 ANF 中的系数 $a_{i_1i_2\ldots i_j}$ 与函数值有如下关系:

$$a_{i_1i_2\ldots i_j}=\bigoplus_{\mathrm{supp}(x)\subseteq\{i_1,i_2,\ldots,i_j\}}f(x),$$

其中,$1\leqslant i_1<i_2<\ldots<i_j\leqslant n$,$1\leqslant j\leqslant n$,集合 $\mathrm{supp}(x_1,\ldots,x_n)=\{i|1\leqslant i\leqslant n,x_i=1\}\subseteq\{1,\ldots,n\}$.

设函数 $f(x)\in B_n$,向量 $a=(a_1,...,a_n)\in F_2^n$.$w(a)$是 a 的 Hamming 重量,i.e.,$w(a)=\#\{i|1\leqslant i\leqslant n,a_i=1\}$.

$w(f(x))$表示 $f(x)$的 Hamming 重量,i.e., $w(f(x))=\#\{x\,|\,x\in F_2^n,f(x)=1\}$.如果 $w(f(x))=2^{n-1}$,我们称 $f(x)$为平衡的.平衡性是布尔函数的一条重要的密码学性质.设 $g(x)\in B_n$,$d(f(x),g(x))=w(f(x)\oplus g(x))$称为 $f(x)$与 $g(x)$之间的距离.

定义 2. n 元布尔函数 $f(x)$的非线性度定义为

$$\mathrm{N}(f)=\min_{g\in A_n}d(f,g).$$

这里,A_n 是全体 n 元仿射函数组成的集合,i.e.,$A_n=\{a_0\oplus a_1x_1\oplus a_2x_2\oplus\ldots\oplus a_nx_n|a_i\in F_2,0\leqslant i\leqslant n\}$.

布尔函数的非线性度是衡量密码体制安全性的一项指标,高非线性度可以抵抗最佳仿射逼近的攻击.

对于布尔函数 $f(x)\in B_n$,其 Walsh 变换定义为

$$W_f(c)=\sum_{x\in F_2^n}(-1)^{f(x)\oplus c\cdot x},$$

其中,$c=(c_1,...,c_n)\in F_2^n$,内积 $c\cdot x=c_1x_1\oplus c_2x_2\oplus\ldots\oplus c_nx_n$,$\Sigma$是实数上的加法,$\oplus$是有限域 F_2 上的加法.

$f(x)$的非线性度也可由表达式给出:

$$\mathrm{N}(f)=2^{n-1}-\frac{1}{2}\max_{c\in F_2^n}|W_f(c)|.$$

定义 3. 设 $f(x)\in B_n$,如果非零布尔函数 $g(x)\in B_n$ 满足 $f(x)\cdot g(x)=0$,则称 $g(x)$是 $f(x)$的零化子.记 AN(f)为 $f(x)$所有的零化子组成的集合.$f(x)$的代数免疫度定义为 AI(f)=deg(h),其中,$h(x)$是集合 AN(f)∪AN($f\oplus1$)中代数次数最小的非零函数.

已知有结论 $\mathrm{AI}(f)\leqslant\left\lceil\frac{n}{2}\right\rceil$ 成立[3],则具有最优代数免疫度 $\left\lceil\frac{n}{2}\right\rceil$ 的布尔函数对代数攻击具有很强的抵抗能力.

2 一种具有最优代数免疫度的布尔函数的构造

在本节中,我们令 n 为偶数,并记

$$W^{<\frac{n}{2}}=\left\{x\,|\,x\in F_2^n,w(x)<\frac{n}{2}\right\},W^{\frac{n}{2}}=\left\{x\,|\,x\in F_2^n,w(x)=\frac{n}{2}\right\},W^{>\frac{n}{2}}=\left\{x\,|\,x\in F_2^n,w(x)>\frac{n}{2}\right\}.$$

令 T,U,S 和 V 为 F_2^n 的不相交子集,其中,$T=\{\alpha_1,\ldots,\alpha_{l_1}\}\subseteq W^{<\frac{n}{2}}$,$U=\{u_1,...,u_{l_2}\}\subseteq W^{\frac{n}{2}}$,$S=\{\beta_1,...,\beta_{l_3}\}\subseteq W^{>\frac{n}{2}}$ 以及 $V=\{v_1,...,v_{l_4}\}\subseteq W^{\frac{n}{2}}$.这里,$l_1\leqslant l_2,l_3\leqslant l_4$.下面我们引入有限域 F_2 上的两个矩阵 $A=(a_{ij})_{l_2\times l_1}$ 与 $B=(b_{ij})_{l_4\times l_3}$,满足:

(1) 对任意的 $1\leqslant i\leqslant l_2,1\leqslant j\leqslant l_1$,如果 $\mathrm{supp}(\alpha_j)\subseteq\mathrm{supp}(u_i)$,则定义 $a_{ij}=1$,否则定义 $a_{ij}=0$;

(2) 对任意的 $1\leqslant i\leqslant l_4,1\leqslant j\leqslant l_3$,如果 $\mathrm{supp}(v_i)\subseteq\mathrm{supp}(\beta_j)$,则定义 $b_{ij}=1$,否则定义 $b_{ij}=0$.

有了上面的概念,我们给出一种具有最优代数免疫度的布尔函数的构造.

定理 1. 设 $f\in B_n$,且

$$f(x)=\begin{cases}1, & x\in W^{<\frac{n}{2}}\cup S\cup U\setminus T\\ a(x), & x\in W^{\frac{n}{2}}\setminus(U\cup V)\\ 0, & x\in W^{>\frac{n}{2}}\cup T\cup V\setminus S\end{cases},$$

其中,$a(x)$是任意一个定义在$W^{\frac{n}{2}}\setminus(U\cup V)$上的布尔值函数.如果上面定义的矩阵$A=(a_{ij})_{l_2\times l_1}$与$B=(b_{ij})_{l_4\times l_3}$均为列满秩矩阵,那么$f$具有最优的代数免疫度.

证明:我们需要证明$\mathrm{AI}(f)=\frac{n}{2}$.

首先证明结论:若函数$g(x)$满足$g(x)\cdot f(x)=0$并且$\deg(g)<\frac{n}{2}$,那么$g(x)=0$.

令$g(x)$的ANF为$a_0\bigoplus_{1\leqslant i\leqslant n}a_ix_i\bigoplus_{1\leqslant i<j\leqslant n}a_{ij}x_ix_j\oplus\ldots\bigoplus_{1\leqslant i_1<i_2<\ldots<i_{\frac{n}{2}-1}\leqslant n}a_{i_1i_2\ldots i_{\frac{n}{2}-1}}x_{i_1}x_{i_2}\ldots x_{i_{\frac{n}{2}-1}}$,系数$a_{i_1i_2\ldots i_j}$与$g(x)$有以下关系:

$$a_{i_1i_2\ldots i_j}=\bigoplus_{\mathrm{supp}(x)\subseteq\{i_1,i_2,\ldots,i_j\}}g(x) \tag{1}$$

这里,$1\leqslant i_1<i_2<\ldots<i_j\leqslant n$且$1\leqslant j<\frac{n}{2}$.

如果我们证明了对任意的$x\in W^{<\frac{n}{2}}$均有$g(x)=0$,那么利用关系式(1)就可以得到$g(x)$的系数都为0,从而$g(x)=0$.由定理中的条件可知:如果$x\in W^{<\frac{n}{2}}\setminus T$,那么$f(x)=1$.从而有

$$g(x)=0 \tag{2}$$

下面我们只需证明对任意的$x\in T$,$g(x)=0$.

因为$\deg(g)<\frac{n}{2}$,以及对任意的$1\leqslant i\leqslant l_2$均有$w(u_i)=\frac{n}{2}$,所以我们有等式$\bigoplus_{\mathrm{supp}(x)\subseteq\mathrm{supp}(u_i)}g(x)=0$.由条件(2)以及矩阵$A$的定义可得$\bigoplus_{j=1}^{l_1}a_{ij}g(\alpha_j)=0$.这样,就得到了$l_2$个关于变量$g(\alpha_j)(1\leqslant j\leqslant l_1)$的齐次线性方程组,且该方程组的系数矩阵为$A$.由于矩阵$A$是列满秩的,所以方程组只有零解.因此,对任意的$x\in T$,$g(x)=0$.这样,我们证明了$f(x)$没有代数次数小于$\frac{n}{2}$的零化子.

其次,我们证明结论:若函数$g(x)$满足$g(x)\cdot(f(x)\oplus 1)=0$并且$\deg(g)<\frac{n}{2}$,那么$g(x)=0$.

此时,只需令$g'(x_1,x_2,\ldots,x_{n-1},x_n)=g(1\oplus x_1,1\oplus x_2,\ldots,1\oplus x_{n-1},1\oplus x_n)$,我们可以用与前面完全类似的方法证明$g'(x_1,x_2,\ldots,x_{n-1},x_n)=0$,从而$g(x_1,x_2,\ldots,x_{n-1},x_n)=0$.这样,我们证明了$f(x)\oplus 1$没有代数次数小于$\frac{n}{2}$的零化子.

上面已经证明f与$f\oplus 1$均没有代数次数$<\frac{n}{2}$的零化子,又由于$\mathrm{AI}(f(x))\leqslant\frac{n}{2}$,最后得到:

$$\mathrm{AI}(f(x))=\frac{n}{2}.$$ □

注:定理1是对文献[7]中第8页出现的构造1的进一步推广,文献[7]中构造1给出的条件相当于给出了可逆的下三角方阵A和可逆的上三角方阵B,是定理1的特例.

如果定理1中的集合T,S,U和V都是F_2^n中的某些轨道的并集,并且$a(x)$在$W^{\frac{n}{2}}\setminus(U\cup V)$中的取值仅与$W^{\frac{n}{2}}\setminus(U\cup V)$中的轨道有关,那么定理1中构造出的函数是旋转对称的.例如,在定理1中,我们取$T=U=\varnothing$和$S=\{(1,1,\ldots,1,1)\}$,取V为由$W^{\frac{n}{2}}$中若干条轨道的并组成集合,易知矩阵B是列满秩的,那么适当调整$a(x)$的取值,

我们可以得到具有最优代数免疫度的旋转对称布尔函数.

推论 1. 设向量 $y_0 \in W^{\frac{n}{2}}$,并且 $G_n(y_0)$是非自共轭轨道.令 $a(x)$是定义在 $W^{\frac{n}{2}} \setminus (G_n(y_0) \cup G_n(\overline{y_0}))$ 上并且满足下面两个条件的布尔值函数:

1. $a(x) = a(\overline{x}), \forall x \in W^{\frac{n}{2}} \setminus (G_n(y_0) \cup G_n(\overline{y_0}))$;
2. $a(x) = a(\rho_n^k(x)), \forall x \in W^{\frac{n}{2}} \setminus (G_n(y_0) \cup G_n(\overline{y_0}))$ 且 $1 \leqslant k \leqslant n$.

那么,函数

$$f(x) = \begin{cases} 1, & x \in W^{<\frac{n}{2}} \cup (1,1,...,1,1) \\ a(x), & x \in W^{\frac{n}{2}} \setminus (G_n(y_0) \cup G_n(\overline{y_0})) \\ 0, & x \in W^{>\frac{n}{2}} \cup G_n(y_0) \cup G_n(\overline{y_0}) \setminus (1,1,...,1,1) \end{cases}$$

是 n 元 RotS 函数并且具有最大的代数免疫度 $\frac{n}{2}$.

3 非线性度

本节我们讨论推论 1 中构造出的函数的非线性度.首先介绍一般函数的非线性度与代数免疫度之间的关系,Lobanov 在文献[8]中给出了一般的 n 元布尔函数的非线性度与代数免疫度之间的关系.

引理 1. $\mathrm{N}(f) \geqslant 2\sum_{i=0}^{\mathrm{AI}(f)-2}\binom{n-1}{i}$.

因此,当 n 为偶数时,如果 $\mathrm{AI}(f) = \frac{n}{2}$,那么 $\mathrm{N}(f) \geqslant 2\sum_{i=0}^{\frac{n}{2}-2}\binom{n-1}{i} = 2^{n-1} - 2\binom{n-1}{\frac{n}{2}-1} = 2^{n-1} - \binom{n}{\frac{n}{2}}$.

设 $\lambda \in F_2^n$,并且 $w(\lambda)=k$,令 $K_i(k,n) = \sum_{w(x)=i}(-1)^{\lambda \cdot x} = \sum_{j=0}^{i}(-1)^j\binom{k}{j}\binom{n-k}{i-j}$.这里,$K_i(k,n)$是 Krawtchouk 多项式.

引理 2. Krawtchouk 多项式有如下性质[7]:

(1) $\sum_{i=0}^{r}K_i(k,n) = K_r(k-1,n-1)$ 对 $0 \leqslant r \leqslant n$ 与 $n,k \geqslant 1$ 成立;

(2) $K_i(k,n)=(-1)^iK_i(n-k,n)$对所有的 $0 \leqslant i,k \leqslant n$ 成立;

(3) $K_{\frac{n}{2}-1}(0,n-1) = \binom{n-1}{\frac{n}{2}-1}$;

(4) $K_{\frac{n}{2}-1}(1,n-1) = \binom{n-1}{\frac{n}{2}-1} \Big/ (n-1)$;

(5) $K_{\frac{n}{2}-1}(2,n-1) = -\binom{n-1}{\frac{n}{2}-1} \Big/ (n-1)$;

(6) $\left|K_{\frac{n}{2}-1}(i,n-1)\right| \leqslant \left|K_{\frac{n}{2}-1}(2,n-1)\right| = \binom{n-1}{\frac{n}{2}-1} \Big/ (n-1)$ 对 $1 \leqslant i \leqslant n-2$ 成立.

定理 2. 设 f 是推论 1 中构造的函数,那么 $\mathrm{N}(f)\geqslant 2^{n-1}-\frac{1}{2}\binom{n}{\frac{n}{2}}-1$.

证明:设 $\lambda\in F_2^n$,令 $t=w(\lambda)$.因为 $G_n(y_0)$是非自共轭轨道,易知存在 $W^{\frac{n}{2}}$ 的子集 A,满足条件:

$$A\supset G_n(y_0),A\cup\overline{A}=W^{\frac{n}{2}}且A\cap\overline{A}=\varnothing.$$

那么,我们有

$$\begin{aligned}W_f(\lambda)&=\sum_{x\in W^{<\frac{n}{2}}\cup(1,1,\ldots,1)}(-1)^{1\oplus\lambda\cdot x}+\sum_{x\in W^{\frac{n}{2}}\setminus(G_n(y_0)\cup G_n(\overline{y_0}))}(-1)^{a(x)\oplus\lambda\cdot x}+\sum_{x\in W^{>\frac{n}{2}}\cup G_n(y_0)\cup G_n(\overline{y_0})\setminus(1,1,\ldots,1,1)}(-1)^{\lambda\cdot x}\\&=\sum_{x\in W^{<\frac{n}{2}}\cup(1,1,\ldots,1)}(-1)^{1\oplus\lambda\cdot x}+\sum_{x\in W^{\frac{n}{2}}\setminus(G_n(y_0)\cup G_n(\overline{y_0}))}(-1)^{a(x)\oplus\lambda\cdot x}+\sum_{x\in W^{<\frac{n}{2}}\cup G_n(y_0)\cup G_n(\overline{y_0})\setminus(0,0,\ldots,0,0)}(-1)^{\lambda\cdot(x\oplus1)}\\&=-\sum_{i=0}^{\frac{n}{2}-1}K_i(t,n)-(-1)^t+\sum_{x\in A\setminus G_n(y_0)}[(-1)^{a(x)\oplus\lambda\cdot x}+(-1)^{a(x)\oplus\lambda\cdot(x\oplus1)}]+\\&\quad(-1)^t\cdot\sum_{i=0}^{\frac{n}{2}-1}K_i(t,n)-(-1)^t+\sum_{x\in G_n(y_0)}[(-1)^{\lambda\cdot x}+(-1)^{\lambda\cdot(x\oplus1)}]\\&=[(-1)^t-1]\cdot\sum_{i=0}^{\frac{n}{2}-1}K_i(t,n)-2(-1)^t+[1+(-1)^t]\sum_{x\in A\setminus G_n(y_0)}(-1)^{a(x)\oplus\lambda\cdot x}+[1+(-1)^t]\sum_{x\in G_n(y_0)}(-1)^{\lambda\cdot x}.\end{aligned}$$

因此,

$$W_f(\lambda)=\begin{cases}-2\sum_{i=0}^{\frac{n}{2}-1}K_i(t,n)+2, & 若t为奇数\\ -2+2\sum_{x\in G_n(y_0)}(-1)^{\lambda\cdot x}+2\sum_{x\in A\setminus G_n(y_0)}(-1)^{a(x)\oplus\lambda\cdot x}, & 若t为偶数\end{cases}.$$

由引理 2,对奇数 t,我们有

$$|W_f(\lambda)|=\left|-2K_{\frac{n}{2}-1}(t-1,n-1)+2\right|\leqslant 2\binom{n-1}{\frac{n}{2}-1}+2=\binom{n}{\frac{n}{2}}+2.$$

对偶数 t,我们有

$$|W_f(\lambda)|\leqslant 2+2\sum_{x\in G_n(y_0)}|(-1)^{\lambda\cdot x}|+2\sum_{x\in A\setminus G_n(y_0)}|(-1)^{a(x)\oplus\lambda\cdot x}|=2+2\#A=2+\binom{n}{\frac{n}{2}},$$

其中,$\#A=\#W^{\frac{n}{2}}/2=\frac{1}{2}\binom{n}{\frac{n}{2}}$.

综上所述,我们得到不等式 $\max_{\lambda\in F_2^n}|W_f(\lambda)|\leqslant 2+\binom{n}{\frac{n}{2}}$.因此,$\mathrm{N}(f)=2^{n-1}-\frac{1}{2}\max_{\lambda\in F_2^n}|W_f(\lambda)|\geqslant 2^{n-1}-\frac{1}{2}\binom{n}{\frac{n}{2}}-1$. □

从定理 2 的结论可以看出,推论 1 中的函数具有较高的非线性度,而且该非线性度的下界与文献[3]中构造出的函数的非线性度在表达式上几乎是相等的.在实际应用中,利用定理 2 的证明过程,我们可以设计出非线性度更大的函数.

4 具有最优代数免疫度的平衡 RotS 函数的构造

到目前为止,还没有关于构造偶数元具有最优代数免疫度的平衡 RotS 函数的文献.下面我们将在 $n=2^d(d>2)$的情况下构造出具有最优代数免疫度的平衡 RotS 函数.在给出我们的构造之前,先介绍一些需要用到的结论.

令 $n=2^d(d>2)$,下面我们考虑 $W^{\frac{n}{2}}$ 中的向量.注意到 $W^{\frac{n}{2}}$ 中向量的周期是 $n=2^d$ 的一个因子,i.e.,所有向量的周期均在集合 $\{2^q|1\leqslant q\leqslant d\}$ 内.用 A_q 表示在 $W^{\frac{n}{2}}$ 中的周期为 2^q 的向量组成的集合,$1\leqslant q\leqslant d$.下面给出集合 A_q 内向量的个数.

命题 1. A_q 内向量的个数为

$$\#A_q=\begin{cases}2, & q=1\\ \binom{2^q}{2^{q-1}}-\binom{2^{q-1}}{2^{q-2}}, & 2\leqslant q\leqslant d\end{cases}.$$

证明:令 $a=(a_1,a_2,...,a_{n-1},a_n)\in W^{\frac{n}{2}}$,如果 a 的周期 $T_n(a)$在集合 $\{2,2^2,2^3,\ldots,2^q\}$ 内,我们有关系式 $a_i=a_{i+2^q}$ $(1\leqslant i\leqslant n)$.此时, $a=(a_1,a_2,a_3,...,a_{2^q},a_1,a_2,a_3,...,a_{2^q},...,a_1,a_2,a_3,...,a_{2^q})$. 因为 $w(a)=\frac{n}{2}$,所以在集合 $\{a_1,a_2,a_3...,a_{2^q}\}$ 内有 2^{q-1} 个 0 和 2^{q-1} 个 1.反过来,如果向量 $b=(b_1,b_2,...,b_{2^q},b_1,b_2,...,b_{2^q},...,b_1,b_2,...,b_{2^q})\in F_2^n$,并且在 $\{b_1,b_2,b_3,...,b_{2^q}\}$ 中有 2^{q-1} 个 0 和 2^{q-1} 个 1,那么 $b\in W^{\frac{n}{2}}$,并且 b 的周期 $T_n(b)$在集合 $\{2,2^2,2^3,\ldots,2^q\}$ 内.

因此,我们得到在 $W^{\frac{n}{2}}$ 内,并且周期在集合 $\{2,2^2,2^3,\ldots,2^q\}$ 内的所有向量的个数为 $\binom{2^q}{2^{q-1}}$.如果 $q=1$,我们有 $\#A_1=\binom{2}{1}=2$;如果 $q\geqslant 2$,由于在 $W^{\frac{n}{2}}$ 内,并且周期在集合 $\{2,2^2,2^3,\ldots,2^{q-1}\}$ 内的所有向量的个数为 $\binom{2^{q-1}}{2^{q-2}}$,所以有 $\#A_q=\binom{2^q}{2^{q-1}}-\binom{2^{q-1}}{2^{q-2}}$. □

注意,包含在 A_q 内的轨道的个数为 $\#A_q/2^q$,下面证明:当 $q>2$ 时,这个数能被 4 整除.首先介绍两个引理,文献[9]给出了下面的两个结论:

引理 3. 若 m 是正整数,p 是素数,则在 $m!$的素因子分解式中,p 的指数为 $\left\lfloor\frac{m}{p}\right\rfloor+\left\lfloor\frac{m}{p^2}\right\rfloor+\left\lfloor\frac{m}{p^3}\right\rfloor+\ldots$,其中,$\lfloor x\rfloor$表示不超过实数 x 的最大整数.

引理 4. 设 n 为正整数,则 $(x_1+x_2+\ldots+x_m)^n=\sum\frac{n!}{n_1!n_2!\ldots n_m!}x_1^{n_1}x_2^{n_2}\ldots x_m^{n_m}$.其中的求和号是对所有满足 $n_1+n_2+\ldots+n_m=n$ 的非负整数序列 $n_1,n_2,\ldots,n_m$ 求和.

命题 2. 如果 $q>2$,那么, $2^{q+2}\left|\left(\binom{2^q}{2^{q-1}}-\binom{2^{q-1}}{2^{q-2}}\right)\right.$.

证明:首先,易验证:当 $q=3$ 和 $q=4$ 时,命题成立.下面我们证明:当 $q\geqslant 5$ 时命题成立.

注意到 $\binom{2^q}{2^{q-1}}$ 是 $(1+x)^{2^q}$ 的展开式中项 $x^{2^{q-1}}$ 的系数,同时,由于 $(1+x)^{2^q}=[(1+x)^2]^{2^{q-1}}=(1+2x+x^2)^{2^{q-1}}$,由引理 4 可知, $(1+2x+x^2)^{2^{q-1}}$ 展开式中的每一项有如下形式:

$$\frac{2^{q-1}!}{a!b!c!}1^c(2x)^a(x^2)^b,$$

其中,整数 a,b,c 满足 $0\leqslant a\leqslant 2^{q-1},0\leqslant b\leqslant 2^{q-1},0\leqslant c\leqslant 2^{q-1},a+b+c=2^{q-1}$,而且该项的代数次数为 $a+2b$,系数为

$\frac{2^a\cdot 2^{q-1}!}{a!b!c!}$.因此,如果某一项的代数次数为 2^{q-1},那么 a,b,c 满足等式:$a+2b=2^{q-1}$,$a+b+c=2^{q-1}$.从这两个等式中我们得到 $b=c$.因此,项 $x^{2^{q-1}}$ 的系数为 $\sum_{\substack{0\leqslant b\leqslant 2^{q-2}\\ a+2b=2^{q-1}}}\frac{2^a\cdot 2^{q-1}!}{a!(b!)^2}$,而且该值为 $\binom{2^q}{2^{q-1}}$.如果 $b=2^{q-2}$,那么 $a=0$.此时,$\frac{2^0\cdot 2^{q-1}!}{0!(2^{q-2}!)^2}=\frac{2^{q-1}!}{(2^{q-2}!)^2}=\binom{2^{q-1}}{2^{q-2}}$.因此,有等式$\binom{2^q}{2^{q-1}}-\binom{2^{q-1}}{2^{q-2}}=\sum_{\substack{0\leqslant b<2^{q-2}\\ a+2b=2^{q-1}}}\frac{2^a\cdot 2^{q-1}!}{a!(b!)^2}$.

下面证明:对于满足 $0\leqslant b<2^{q-2}$ 与 $a+2b=2^{q-1}$ 的整数 a 与 b,有 $2^{q+2}\left|\frac{2^a\cdot 2^{q-1}!}{a!(b!)^2}\right.$.

记 r_a 是 $\frac{2^a\cdot 2^{q-1}!}{a!(b!)^2}$ 的素因子分解式中 2 的次幂,由引理 3 可知,$a!$的素因子分解式中 2 的次幂为

$$\left\lfloor\frac{a}{2}\right\rfloor+\left\lfloor\frac{a}{2^2}\right\rfloor+\left\lfloor\frac{a}{2^3}\right\rfloor+\ldots\leqslant\frac{a}{2}+\frac{a}{2^2}+\frac{a}{2^3}+\ldots\leqslant a.$$

$b!$的素因子分解式中 2 的次幂为

$$\left\lfloor\frac{b}{2}\right\rfloor+\left\lfloor\frac{b}{2^2}\right\rfloor+\left\lfloor\frac{b}{2^3}\right\rfloor+\ldots\leqslant\left\lfloor\frac{2^{q-2}-1}{2}\right\rfloor+\left\lfloor\frac{2^{q-2}-1}{2^2}\right\rfloor+\left\lfloor\frac{2^{q-2}-1}{2^3}\right\rfloor+\ldots=(2^{q-3}-1)+(2^{q-4}-1)+\ldots+(2-1)=2^{q-2}-q+1.$$

$2^{q-1}!$的素因子分解式中 2 的次幂为

$$\left\lfloor\frac{2^{q-1}}{2}\right\rfloor+\left\lfloor\frac{2^{q-1}}{2^2}\right\rfloor+\left\lfloor\frac{2^{q-1}}{2^3}\right\rfloor+\ldots=2^{q-2}+2^{q-3}+\ldots+2+1=2^{q-1}-1.$$

因此,$r_a\geqslant a+2^{q-1}-1-a-2(2^{q-2}-q+1)=2q-3\geqslant q+2$,其中,$q\geqslant 5$.从而有 $2^{q+2}\left|\left(\binom{2^q}{2^{q-1}}-\binom{2^{q-1}}{2^{q-2}}\right)\right.$. □

由命题 2 可知,当 $q>2$ 时,包含在 A_q 内所有轨道的个数能被 4 整除.下面我们对 A_q 给出更具体的描述.

例如,当 $q=1$ 时,$\#A_1=2$.包含在 A_1 中的向量的周期为 $T_n=2^1=2$,这些向量在$\#A_1/T_n=2/2=1$ 个轨道内,且

$$A_1=\{(1,0,1,0,\ldots,1,0,1,0),(0,1,0,1,\ldots,0,1,0,1)\}.$$

当 $q=2$ 时,$\#A_2=\binom{2^2}{2}-\binom{2}{1}=4$,$A_2$ 中每个向量的周期为 $T_n=2^2=4$,A_2 内轨道的个数为$\#A_2/T_n=4/4=1$,并且

$$A_2=\{(1,1,0,0,1,1,0,0,\ldots,1,1,0,0,1,1,0,0),(0,1,1,0,0,1,1,0,\ldots,0,1,1,0,0,1,1,0),$$
$$(0,0,1,1,0,0,1,1,\ldots,0,0,1,1,0,0,1,1),(10,0,1,1,0,0,1,\ldots,10,0,1,1,0,0,1)\}.$$

当 $q\geqslant 3$ 时,根据对 A_q 中的轨道按自共轭和非自共轭分类可知,A_q 有如下的轨道分解:

$$A_q=\bigcup_{i=1}^{s_q}(G_n(u_i^{(q)})\cup G_n(\overline{u_i^{(q)}}))\bigcup_{j=1}^{t_q}G_n(v_j^{(q)}),$$

其中,$u_i^{(q)},v_j^{(q)}\in A_q$,$\bigcup_{j=1}^{t_q}G_n(v_j^{(q)})$ 为 A_q 内所有自共轭轨道的集合,$\bigcup_{i=1}^{s_q}(G_n(u_i^{(q)})\cup G_n(\overline{u_i^{(q)}}))$ 为 A_q 内所有非自共轭轨道的集合.下面我们给出 t_q 的大小.

命题 3. 设 $q\geqslant 3$,则 A_q 中自共轭轨道的个数为 $2^{2^{q-1}-q}$.

证明:令 $G_n(a)$是包含在 A_q 内的一条自共轭轨道,这里,$a=(a_1,\ldots,a_{2^q},a_{2^q+1},\ldots,a_n)\in A_q$ 且 $T_n(a)=2^q$.显然,a 由 $a_1,\ldots,a_{2^q}$ 决定.因为 $G_n(a)=G_n(\overline{a})$,所以存在一个整数 $m(0<m<2^q)$使得$(a_1,\ldots,a_n)=(a_{1+m}\oplus 1,\ldots,a_{n+m}\oplus 1)$.从而有

$$(a_1,\ldots,a_n)=(a_{1+m}\oplus 1,\ldots,a_{n+m}\oplus 1)=((a_{1+m+m}\oplus 1)\oplus 1,\ldots,(a_{n+m+m}\oplus 1)\oplus 1)=(a_{1+2m},\ldots,a_{n+2m}).$$

又由于 $T_n(a)=2^q$,我们有 $2^q|2m$ 成立.注意到 $0<m<2^q$,可得 $m=2^{q-1}$.因此,对任意的 $1\leqslant i\leqslant 2^{q-1}$,均有 $a_{i+2^{q-1}}=a_i\oplus 1$ 成立.最后可知,a 仅由 $a_1,\ldots,a_{2^{q-1}}$ 决定.反过来,若向量 $a=(a_1,\ldots,a_{2^{q-1}},a_{2^{q-1}+1},\ldots,a_n)\in F_2^n$ 满足条件:$a_{i+2^{q-1}}=a_i\oplus 1$,$1\leqslant i\leqslant 2^{q-1}$,且 $a_{i+2^q}=a_i$,$1\leqslant i\leqslant n$,那么,a 的周期为 $T_n(a)=2^q$.这是因为此时 $T_n(a)|2^q$,且 $a_1\neq a_{1+2^{q-1}}$.

因此,A_q 内满足 $G_n(a)=G_n(\bar{a})$ 的向量 a 的个数为 $2^{2^{q-1}}$.注意到,A_q 的每条轨道内有 2^q 个向量,因此,包含在 A_q 内的自共轭轨道的个数为 $t_q=2^{2^{q-1}}/2^q=2^{2^{q-1}-q}$. □

下面我们给出 A_q 的另一种不相交子集的分解.易知,当 $q>3$ 时有 $4|t_q$.注意,A_q 中的轨道数,我们有等式 $2s_q+t_q=\#A_q/2^q$,从中解得 $s_q=\#A_q/2^{q+1}-t_q/2$.由命题 1~命题 3 可知,当 $q>3$ 时 s_q 为偶数.此时我们令

$$B_q=\bigcup_{i=1}^{\frac{s_q}{2}}(G_n(u_i^p)\cup G_n(\overline{u_i^p}))\bigcup_{j=1}^{\frac{t_q}{2}}G_n(v_j),\ C_q=\bigcup_{i=\frac{s_q}{2}+1}^{s_q}(G_n(u_i^p)\cup G_n(\overline{u_i^p}))\bigcup_{j=\frac{t_q}{2}+1}^{t_q}G_n(v_j).$$

那么,$A_q=B_q\cup C_q$,且 $B_q\cap C_q=\varnothing$.显然,B_q 与 C_q 有相同的轨道数,因此它们含有向量的个数相等.我们有

$$\#B_q=\frac{1}{2}\#A_q=\frac{1}{2}\left(\binom{2^q}{2^{q-1}}-\binom{2^{q-1}}{2^{q-2}}\right).$$

当 $q=3$ 时,$\#A_3=\binom{2^3}{2^2}-\binom{2^2}{2}=64,t_3=2^{2^{3-1}-3}=2,s_3=\#A_3/2^4-t_3/2=3$.令

$$B_3=\bigcup_{i=1}^{2}(G_n(u_i^3)\cup G_n(\overline{u_i^3})),\ C_3=G_n(u_3^3)\cup G_n(\overline{u_3^3})\bigcup_{j=1}^{2}G_n(v_j^q),$$

那么,$A_3=B_3\cup C_3$,$B_3\cap C_3=\varnothing$,并且 $\#B_3=\frac{1}{2}\#A_3=32$.

有了上面的基础,我们构造下面的平衡函数.

定理 3. 令 $n=2^d$ 且 $d>2$,那么函数

$$f(x)=\begin{cases}1,\ x\in W^{<\frac{n}{2}}\cup(1,1,...,1,1)\cup A_1\bigcup\limits_{2<q\leqslant d}B_q\\ 0,\ x\in W^{>\frac{n}{2}}\setminus(1,1,...,1,1)\cup A_2\bigcup\limits_{2<q\leqslant d}C_q\end{cases}$$

是 n 元具有最优代数免疫度的平衡 RotS 函数.

证明:由推论 1 可知,$f(x)$是具有最优代数免疫度的 RotS 函数,又因为

$$\begin{aligned}\#\{x\mid x\in F_2^n,f(x)=1\}&=\sum_{i=0}^{\frac{n}{2}-1}\binom{n}{i}+1+2+\frac{1}{2}\sum_{j=3}^{d}\left(\binom{2^j}{2^{j-1}}-\binom{2^{j-1}}{2^{j-2}}\right)\\&=2^{n-1}-\frac{1}{2}\binom{n}{\frac{n}{2}}+3+\frac{1}{2}\left(\binom{2^d}{2^{d-1}}-\binom{4}{2}\right)\\&=2^{n-1}.\end{aligned}$$

即 $w(f)=2^{n-1}$.因此,$f(x)$是平衡的. □

由定理 2 可知,定理 3 中的函数也具有较高的非线性度.

5 结束语

在本文中,我们给出了一种具有最优代数免疫度的偶数元布尔函数的构造,并且还给出了一种具有最优代数免疫度的平衡偶数元 RotS 函数的构造.因为我们的函数具有最优的代数免疫度,所以这些函数对代数攻击有很强的抵抗能力.同时,定理 3 中给出的函数还具有较高的非线性度,能够在一定程度上抵抗线性攻击.

References:

[1] Stănică P, Maitra S. Rotation symmetric Boolean functions-count and cryptographic properties. Discrete Applied Mathematics, 2008,156(10):1567−1580. [doi: 10.1016/j.dam.2007.04.029]

[2] Filiol E, Fontaine C. Highly nonlinear balanced Boolean functions with a good correlation immunity. In: Nyberg K, ed. Advances in Cryptology—EUROCRYPT'98. LNCS 1403, Heidelberg: Springer-Verlag, 1998. 475−488.

[3] Carlet C. Algebraic immunity for cryptographically significant Boolean functions: analysis and construction. IEEE Trans. on Information Theory, 2006,52(7):3105−3121. [doi: 10.1109/TIT.2006.876253]

[4] Li N, Qi WF. Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity. IEEE Trans. on Information Theory, 2006,52(5):2271−2273. [doi: 10.1109/TIT.2006.872977]

[5] Li N, Qi WF. Construction and count of Boolean functions of an odd number of variables with maximum algebraic immunity. Science in China (Series F: Information Science), 2007,50(3):307−317 (in Chinese with English abstract). [doi: 10.1007/s11432-007-0027-4]

[6] Sarkar S, Maitra S. Construction of rotation symmetric Boolean functions with maximum algebraic immunity an odd number of variables. In: Boztas S, Lu HF, eds. Proc. of the 17th Symp. on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. LNCS 4851, Heidelberg: Springer-Verlag, 2007. 271−280.

[7] Carlet C, Zeng XY, Li CL, Hu L. Further properties of several classes of Boolean functions with optimum algebraic immunity. Designs, Codes and Cryptography, 2009,52(3):303−338. [doi: 10.1007/s10623-009-9284-0]

[8] Lobanov MS. Exact relation between nonlinearity and algebraic immunity. Discrete Mathematics and Applications, 2006,16(5):453−460. [doi: 10.1515/156939206779238418]

[9] Kisačanin B. Mathematical Problems and Proofs: Combinatorics, Number Theory, and Geometry. New York: Plenum Press, 1998. 67−68, 97−98.

附中文参考文献:

[5] 李娜,戚文峰.具有最优代数免疫的奇数元 Boole 函数.中国科学(E 辑:科学信息),2007,50(3):307−317.

孟强(1982－),男,山东枣庄人,博士生,主要研究领域为密码学,编码理论.

陈鲁生(1962－),男,博士,教授,博士生导师,主要研究领域为密码学,信息论,编码理论.

符方伟(1963－),男,博士,教授,博士生导师,主要研究领域为密码学,信息论,编码理论.